STATE OF VERMONT
Agency of Administration

Standard **STC** **STATE TECHNOLOGY COLLABORATIVE**	**ORIGINAL POLICY ADOPTED BY STC** **DATE**	**ORIGINAL POLICY NUMBER**
	EFFECTIVE DATE	**ASSOCIATED DOCUMENTATION** 0502.012005 Malicious Software Protection for Desktops & Servers

STATUTORY REFERENCE
OR OTHER AUTHORITY: **SOV Personnel Policies and Procedures Number 11.7 -** ELECTRONIC COMMUNICATIONS AND INTERNET USE

APPROVAL DATE:

APPROVED BY: **Secretary of Administration**

STANDARD TITLE: **Anti-Virus Software Protection for Desktops & Servers**

STANDARD STATEMENT: **Anti-virus applications protecting PC based systems are one of the most effective protections against malware. Anti-virus protection is the basic level of protection and is covered by the first standard associated with the malware policy. As malware continues to evolve, future standards associated with the malware policy will likely be adopted.**

All PC based computers in use by the State of Vermont or accessing non-public SOV resources must have current, active anti-virus protection meeting these standards.

STANDARD:

Anti-virus (AV) applications must be in place to protect:

- all agency or department PC-based computers (includes, but is not limited to, desktop computers, laptop computers, proxy servers, and any file and print servers),
- all third-party relationships (business, government or individuals) who access non-public State of Vermont resources,
- centralized e-mail gateways that provide mail services to or into the State of Vermont,

The AV application must be:

- currently supported by the manufacturer,
- kept up to date,
- a standard product offered under state contract,
- installed and configured to run automatically,
- providing real time protection,
- scanning removable media,
- configured to run full system scans at least once a week, and
- configured to have its virus patterns updated on a bi-weekly or shorter schedule.

All State of Vermont Agencies or Departments must have:

- a definitive, written process in place to allow for real-time updating of virus pattern files during times of a specific threat.
- an operational procedure in place that ensure anti-virus software is installed and operational,
- an operational process in place that ensures its computers are verified as virus-free,
- an operational process in place that removes virus-infected computers from the network until they are verified as virus-free (for further information refer to the CSIRT incident response procedures).

- a clear understanding of employee responsibilities for complete compliance with this standard.
- IT contacts designated or a process defined for handling violation notifications that are passed through the head of the agency.
- A procedure in place to allow DI+I staff to audit the agency's systems.